UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/975,815	10/11/2001	Neal A. Krawetz	10019968-1	9182

7590 11/30/2005

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, CO 80527-2400

EXAMINER	
COLIN, CARL G	

ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 11/30/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/975,815	KRAWETZ, NEAL A.	
	Examiner	Art Unit	
	Carl Colin	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *19 September 2005* .

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-34* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-34* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *11 October 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other:

DETAILED ACTION

Response to Arguments

1. In response to communications filed on 9/19/2005, applicant amends claim 33. The following claims 1-34 are presented for examination.

2. In response to communications filed on 9/19/2005, the objection to the specification has been withdrawn with respect to the amendment to the specification.

3. Applicant's remarks, pages 9-15, filed on 9/19/2005, with respect to the rejection of claims 1-34 have been fully considered but they are not persuasive. With regard to independent claim 1, Applicant argues that Aucsmith does not disclose an identification key associated with the sender. As indicated in the last Office Action, the identification mark of Aucsmith is related to a composite key that also meets the recitation of private key of the sender as explained in column 5 and column 6, lines 38-52); also as disclosed in column 4, lines 47-51, the composite key identifies the origin of the process (the sender) that meets the recitation of an identification mark or identification key associated with the sender. Applicant argues that the combination of Aucsmith and Roberts does not disclose decrypting the encrypted data using a private key associated with a sender. Upon further consideration, Aucsmith discloses either alone or in combination with Roberts a composite key that also meets the recitation of private key associated with a sender as mentioned above, and further discloses that the decryption unit decrypts the encrypted data using the composite key (column 6, lines 30-65). Independent claims 19 and 27

recite similar limitations. Furthermore, although not explicitly stated in Aucsmith "generating a hash key using the character string and a private key wherein the character string is randomly generated", the process described by Aucsmith in column 5 is very well known in the art for generating a hash key using the character string and a private key wherein the character string sometimes used as a "salt" is randomly generated as mentioned in Kaufman (Applicant's disclosure). Therefore, applicant's claimed invention is considered obvious over the prior art Aucsmith either alone or in combination with the cited art. It remains the examiner's position that claims 1-34 are still rejected for at least the reasons cited above.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4.1 **Claims 1-34** are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent 5,757,915 to **Aucsmith et al** in view of US Patent Publication US 2002/0094085 to **Roberts**.

4.2 **As per claims 1-2, 4, 8, 12, 14-15, 19, 22-25, 28, 31-33, Aucsmith et al** substantially teaches a system for secure data transmission, comprising the following modules and parts (column 8, lines 1-40 and figures 2, 4, and 5): a processor and a memory coupled to the processor (column 8, lines 1-10 and figure 5); encryption/decryption modules (fig. 2, 4, and 5) comprising an encryption engine stored in the memory and executable by the processor, the encryption engine adapted to encrypt the data using the hash key (column 8, lines 1-40 and column 5, line 65 though column 6, line 7); and wherein the processor is adapted to transmit the encrypted data, an identification key related to the private key, and the character string to a recipient (column 5, line 5 though column 6, line 7 and column 6, lines 39-52), and further discloses generation module and signature generator units stored in the memory and executable by the processor that meet the recitation of string generator and hashing engine, for performing cryptographic key hashed functions and generating cryptographic key hashed values (column 5). **Aucsmith et al** further discloses any cryptographic method for generating hash key (column 5, lines 5-32). **Aucsmith et al** discloses generating keyed hash value for encrypting the data but does not explicitly disclose generating a hash key using the character string and a private key wherein the character string is randomly generated. However, **Roberts** in an analogous art teaches a method and system for generating encryption keys using random bit generators. **Roberts** discloses transmitting a random seed that meets the recitation of a character string to a recipient (page 2, paragraph 0022) and further discloses a master key is used along with a random bit sequence called a seed into a one-way hash algorithm to generate an encryption/decryption key (page 1, paragraphs 008-0010 and page 4, paragraphs0040-0043) that meets the recitation of a hash engine adapted to hash the character string and a private key to

generate a hash key used for encryption and decryption. The advantage is that changing the seed periodically also changes the key periodically, thus even if an eavesdropper manages to identify the key, and the eavesdropper will only have access to the secure communications until the key is changed. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of key generation of **Aucsmith et al** to integrate the concept of generating encryption/decryption keys by hashing a random seed with a private key as taught by **Roberts** to make it more difficult for eavesdroppers to identify the key (page 1, paragraphs 008-0010). The motivation to do so is given by **Roberts** who teaches that changing the seed periodically also changes the key periodically, thus even if an eavesdropper manages to identify the key, and the eavesdropper will only have access to the secure communications until the key is changed; this method makes it more difficult for eavesdroppers to identify the key (page 1, paragraphs 008-0010).

As per claims 3, 20, and 29, the combination of **Aucsmith et al** and **Roberts** discloses the limitation of comprising a signature engine stored in the memory and executable by the processor, the signature engine adapted to generate a signature using the hash key and the data, the processor further adapted to transmit the signature to the recipient (**Aucsmith et al**, column 5, line 59 through column 6, line 7; and column 6, line 53 through column 7, line 10).

As per claim 21, the combination of **Aucsmith et al** and **Roberts** discloses the limitation of wherein the recipient is adapted to decrypt the encrypted data and verify the signature using the decrypted data (**Aucsmith et al**, column 8, line 52 through column 9, line 18).

As per claims 6, 13, and 26, the combination of **Aucsmith et al** and **Roberts** discloses the limitation of wherein the recipient is adapted to access a relational database associating the identification key with the private key (**Aucsmith et al**, column 7, lines 29-50) and decrypt the encrypted data using the private key and the character string (**Roberts,** page 1, paragraph 0011). Therefore, these claims are rejected on the same rationale as the rejection of claims 1 and 19.

Claim 27 contains the same limitations as claims 19 and 26 and therefore is rejected on the same rationale as the rejection of claims 19 and 26.

As per claims 16, 17, 30, the combination of **Aucsmith et al** and **Roberts** discloses a hashing engine stored in the memory and executable by the processor, the hashing engine adapted to generate a hash key using the private key and the character string as discussed in claims 1 and 19 above; and a signature engine stored in the memory and executable by the processor, the signature engine adapted to verify a signature received from the sender using the hash key and the decrypted data (**Aucsmith et al**, column 8, line 52 through column 9, line 18). Therefore, these claims are rejected on the same rationale as the rejection of claims 1 and 19.

As per claims 5, 7, 9-11, 18, and 34, the combination of **Aucsmith et al** and **Roberts** discloses the limitation of generating a signature using the hash key and the data; transmitting the signature to the recipient (**Aucsmith et al**, column 5, line 59 through column 6, line 7; and column 6, line 53 through column 7, line 10); determining the private key at the recipient using

the identification key (**Aucsmith et al**, column 7, lines 29-50); determining the hash key at the recipient using the private key and the character string (**Roberts,** page 1, paragraph 0011 and page 2, paragraph 0022); decrypting the encrypted data at the recipient using the hash key (**Roberts,** page 1, paragraph 0011); and verifying the signature at the recipient using the hash key and the decrypted data (**Aucsmith et al**, column 8, line 52 through column 9, line 18). Therefore, these claims are rejected on the same rationale as the rejection of claims 1 and 19.

Conclusion

5. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a). A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

5.1 The prior art made of record and not relied upon is considered pertinent to applicant's disclosure as the art discloses secure data communications using hashing, signature, encryption message authentication and verification.

US Patent Publication: US 2001/0002929 Mache

US Patents: 6,058,188 Chandersekaran et al ; 5,689,567 Miyauchi ; 5,987,133 Aisaka ; 5,701,343 Takashima et al. ; 5,757,915 Kaufman et al.

5.2 Any inquiry concerning this communication or earlier communications from the examiner should be directed to Carl Colin whose telephone number is 571-272-3862. The examiner can normally be reached on Monday through Thursday, 8:00-6:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Carl Colin
Patent Examiner
November 25, 2005

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100